ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
INFORMATION TECHNOLOGY, COMPUTER SCIENCE, AND MANAGEMENT



УДК 519.7 DOI 10.12737/16054

Модель организации защищенного документооборота на базе распределенной передачи данных с аутентификацией*

В. М. Деундяк[1], С. Б. Попова[2]**
[1]Южный федеральный университет, ФГНУ НИИ «Спецвузавтоматика», г. Ростов-на-Дону, Российская Федерация
[2]Южный федеральный университет, г. Ростов-на-Дону, Российская Федерация

Secure document management model based on distributed data transmission with authentication***

V. M. Deundyak[1], S. B. Popova[2]**
[1]Southern Federal University, Research Institute "Spetsvuzavtomatika", Rostov-on-Don, Russian Federation
[2]Southern Federal University, Rostov-on-Don, Russian Federation

Организация защищенного документооборота является предметом данного исследования. Его цель — повышение надежности передачи данных. Задача работы — построение надежной модели организации защищенного документооборота с аутентификацией. Для решения указанной задачи применяется метод распределенной передачи данных, который позволяет за счет использования нескольких каналов значительно уменьшить вероятность несанкционированного доступа к информации и возможности ее модификации. В качестве результата работы представлена модель организации защищенного документооборота на основе двухканального алгоритма шифрования MV 2 и базовых шифров AES и RC4. Предусмотрена замена базовых шифров и учтена потребность использования ассоциированных данных, которые должны оставаться открытыми, но быть аутентифицированными вместе с основной зашифрованной информацией. Построенная модель решает поставленную задачу, а программная реализация, разработанная на языке C++ с использованием библиотеки NTL, может быть применена на практике. Область применения полученных результатов — защита коммерческого документооборота.

Ключевые слова: электронный документооборот, конфиденциальность информации, целостность, аутентификация, распределенная защита, ассоциированные данные.

The present research subject is the secure document management. Its purpose is increasing the reliability of the data transmission. The research problem is the construction of a reliable model of the secure document management with authentication. The distributed data transmission technique which allows – using multiple channels – reduce significantly the risk of the unauthorized access to the information, and the possibilities of its modification, is used to solve this problem. The research result is a secure document management model based on the dual-link MV2 cryptoalgorithm, and AES and RC4 underlying ciphers. The replacement of the basic ciphers is provided, and the need of the additional associated data which must remain open, but be authenticated with the basic encrypted information is considered. The model constructed solves the original problem, and the software implementation developed in C ++ using NTL library can be applied in practice. The application field of the results obtained is the commercial document management protection.

Keywords: electronic document management, information confidentiality, integrity, authentication, distributed protection, associated data.

Введение и постановка задачи. В настоящее время система электронного документооборота получила широкое распространение, стремительно увеличивается объем соответствующих документов [1]. Очевидно, что растет необходимость в обеспечении их защиты, контроле их целостности. Для достижения указанных целей применяются различные криптографические методы, которые позволяют обеспечивать конфиденциальность обрабатываемых данных, а также осуществлять проверку их целостности, т. е. отслеживать факт случайного искажения или несанкционированной модификации [2].

*Работа выполнена в рамках инициативной НИР.
**E-mail: vl.deundyak@gmail.com, svetyla92@mail.ru
***The research is done within the frame of the independent R&D.

Для проверки целостности используются методы аутентификации. Следует отметить, что аутентификация актуальна не только для зашифрованных текстов, но и для открытых данных, называемых ассоциированными. Например, для заголовков сетевых пакетов, которые должны быть не зашифрованы, но аутентифицированы с передаваемой зашифрованной полезной нагрузкой [3–5]. С этой целью применяются методы передачи по распределенным закрытым или частично закрытым сетям. Поэтому особый интерес представляют методы многоканальной криптографии, использование которых позволяет разбивать защищаемую информацию на несколько частей [6–11]. Очевидно, что при отсутствии одной из частей восстановление, анализ или модификация данных невозможны. Таким образом, обеспечивается более высокий уровень защиты данных.

Итак, научный и практический интерес представляют методы распределенной передачи данных, позволяющие одновременно шифровать и аутентифицировать как зашифрованные, так и ассоциированные данные. В связи с этим актуальной задачей является создание простой, надежной и эффективной модели организации защищенного документооборота с аутентификацией. В представленной статье описана такая модель, основанная на схеме двухканального шифрования MV 2.

Необходимые сведения о схеме двухканального шифрования MV 2. Схема двухканального шифрования MV 2 разработана в [7–8].

Рассмотрим алгоритм зашифрования, представленный на рис. 1. В алгоритме используется ключ, длина которого может равняться 128, 256, 512 или 1024 битов.

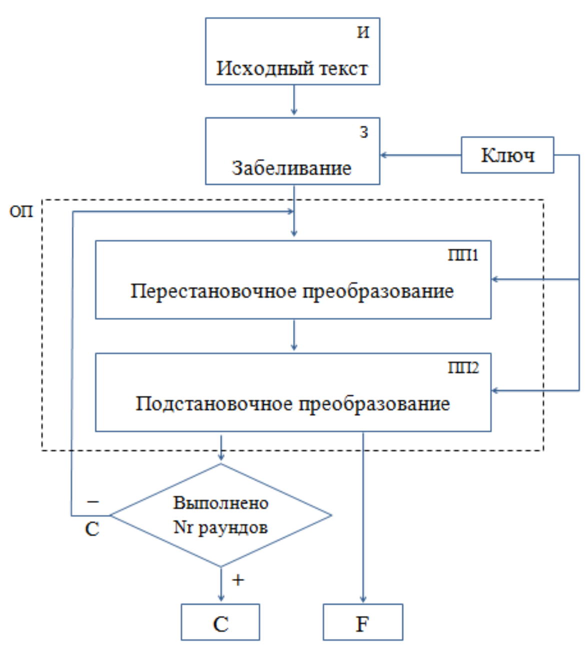


Рис. 1. Схема зашифрования алгоритма MV 2

Изначально данные, которые требуется зашифровать, подаются в блок «И» (исходный текст). Из этого блока они поступают в блок «З» (забеливание), где происходит преобразование данных — их начальная рандомизация. Для забеливания к исходному тексту применяется поточный шифр, что позволяет разрушить статистические зависимости в тексте. В качестве такого шифра используется RC4 [6]. Отметим, что при необходимости RC4 может быть заменен другим потоковым шифром с близкими параметрами.

Забеленный текст поступает на вход основного процесса (ОП) шифрования, состоящего из нескольких раундов. Всего выполняется *Nr* раундов преобразований. В каждом раунде входные данные подвергаются преобразованию: перестановочному (блок «ПП1») и подстановочному MV 2 (блок «ПП2»). В качестве перестановочного преобразования в модели используется алгоритм AES [12], который может быть заменен на другой блочный шифр с аналогичными характеристиками. Подстановочное преобразование осуществляется с использованием специальных подстановочных таблиц MV 2-преобразований, которые заменяют строки исходного текста фиксированной длины парой строк переменной меньшей длины [7]. При зашифровании остаток С, полученный на выходе блока «ПП2», отправля-

ется на вход следующего раунда преобразований в блок «ПП1». При этом с каждым раундом дополнительная информация, необходимая для обеспечения обратимости MV 2-преобразований (флаг), накапливается в F. Остаток C, полученный на последнем раунде преобразований, называется информационным ядром. Пара шифртекстов C и F образуют выход алгоритма зашифрования.

Таким образом, алгоритм зашифрования обеспечивает разбиение входной конфиденциальной информации на две части — C и F, которые подаются на вход двух открытых каналов. При расшифровании две части зашифрованного текста проходят Nr раундов обратных преобразований основного процесса (ОП). После этого снимается забеливание и тем самым восстанавливаются исходные данные.

Модель защищенного документооборота с аутентификацией. В разработанной модели зашифрованные данные передаются по двум каналам связи. При этом наряду с зашифрованием исходных данных осуществляется также и одновременная их аутентификация (рис. 2).

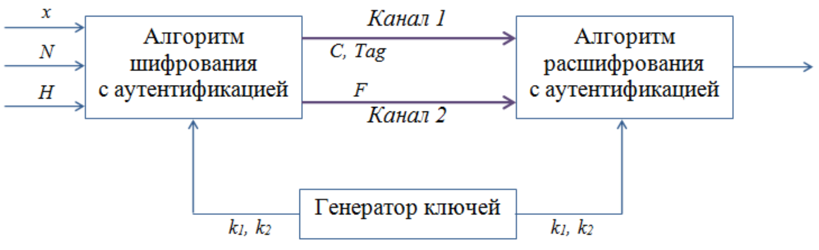


Рис. 2. Общая схема модели

Рассмотрим представленную схему более детально. На вход алгоритма зашифрования с аутентификацией поступают данные трех типов:

— x — данные для зашифрования и аутентификации;

— N — уникальный вектор из n битов, называемый нонсом, который используется один раз в течение жизни ключа;

— H — ассоциированные данные.

Кроме того, на вход алгоритма от генератора ключей поступают также следующие величины:

— k_1 — ключ длины n для алгоритмов зашифрования/расшифрования,

— k_2—ключ длины n для алгоритма аутентификации.

Данные, полученные на выходе алгоритма зашифрования с аутентификацией, отправляются по двум каналам. По первому каналу пересылается первый шифртекст C (остаток) и тег аутентификации Tag, а по второму каналу — второй шифртекст F (флаги). Алгоритм расшифрования с аутентификацией расшифровывает пришедшие по каналам шифртексты C и F. По расшифрованным данным вычисляется тег аутентификации. Аутентификация считается пройденной, если пришедший по каналу вместе с шифртекстами тег аутентификации совпадает с тегом, полученным после работы алгоритма расшифрования. При этом на выходе алгоритма расшифрования с аутентификацией будут получены исходные данные x. В противном случае в качестве результата выдается сообщение об ошибке.

Теперь рассмотрим подробнее работу входящих в схему алгоритмов зашифрования и расшифрования. Разделение на два канала осуществляется с помощью MV 2 (рис. 1). В MV 2 проводится несколько раундов преобразований. Поэтому в построенном алгоритме зашифрования с аутентификацией также выполняется несколько раундов. Следовательно, достаточно рассмотреть работу одного раунда (рис. 3), которая делится на две части — зашифрование (левая часть схемы) и аутентификация (правая часть).

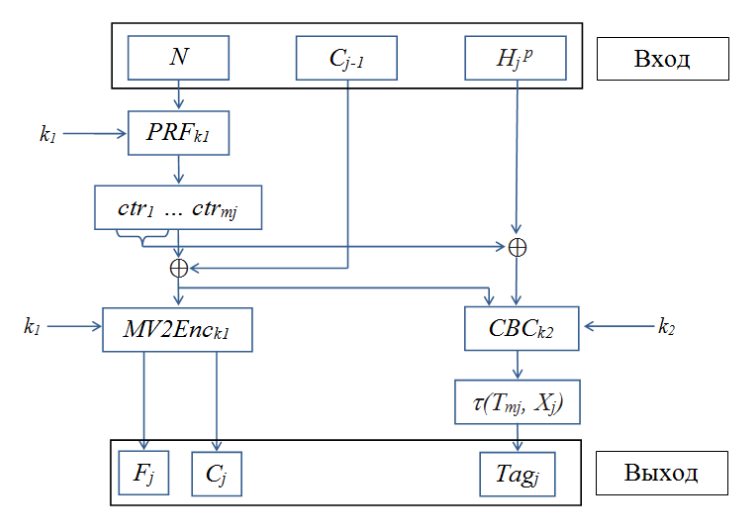


Рис. 3. Схема зашифрования с аутентификацией для j-го раунда

Перед началом зашифрования из n-битного ключа k_1 генерируется 32 вспомогательных ключа по 256 байтов. Предположим, что $n = 128$. Эти ключи представляют собой 32 таблицы подстановочного преобразования [7]. В начале каждого раунда алгоритма MV 2 случайным образом происходит выбор номера таблицы. Обозначим через N_j номер таблицы MV 2-преобразования на j-м раунде:

$$j \in [1, Nr],$$

где Nr — число раундов алгоритма MV 2.

Поступающее на вход раунда зашифрования сообщение C_{j-1} разбивается на блоки, размер которых равен n битов. Если размер последнего блока меньше n, он дополняется до n битов. Для первого раунда $C_0 = x$. Нонс N изначально зашифровывается с помощью псевдослучайной функции на ключе k_1:

$$ctr_1 = PRF_{k1}(N).$$

Из полученного значения ctr_1 вычисляется набор счетчиков:

$$ctr_i = PRF_{k1}(ctr_1 + i - 1),$$

где $i \in [2, m_j]$.

Счетчики суммируются по модулю 2 с зашифровываемым на данном раунде текстом C_{j-1}:

$$S_i = ctr_{i+1} \oplus C_{j-1i},$$

где C_{j-1i} — i-й блок C_{j-1}.

Для получения остатка и флага на j-м раунде к S_i алгоритм MV 2 применяется следующим образом:

$$(c_i, f_i) = MV\,2Enc_{k1}(S_i),$$

где c_i и f_i — соответственно остаток и флаг для i-го блока сообщения C_{j-1i}.

Остаток на j-м раунде C_j получается путем битовой конкатенации значений c_i, а флаг F_j — с помощью битовой конкатенации флагов f_i, $i \in [1, m_j]$, где m_j — число n-битных блоков в C_{j-1}. Остаток C_j отправляется на вход следующего раунда для последующего сжатия, а флаги F_j с каждого раунда накапливаются. В итоге после Nr раундов преобразований получается пара

$$C = C_{Nr},\ F = F_{Nr} \ldots F_1.$$

На этом этапе завершается зашифрование данных.

Проверка целостности осуществляется с помощью кодов аутентификации сообщения. При выработке тега аутентификации для j-го раунда используется режим работы CBC некоторого блочного шифра [13]. На основе этого режима строится последовательность действий, в которой каждый новый зашифрованный блок зависит от результата зашифрования предыдущего. Такая связь дает возможность получить тег аутентификации сообщения, поскольку изменение даже одного бита открытого текста влечет за собой непредсказуемое изменение выходного зашифрованного блока. В качестве блочного шифра для выработки тега аутентификации выбран блочный шифр AES [12].

Опишем процесс получения тега. До начала применения AES необходимо произвести следующие вычисления. Положим $q = |H| / Nr$ и вычислим

$$H_j^p = (0^1, 0^2, \ldots, 0^{p-1}, H^{(j-1)q}, H^{(j-1)q+1}, \ldots, H^{jq-1}, 0^{p+q}, \ldots, 0^n),$$

где 0^i означает, что i-й бит строки H_j^p равен 0; H^k — k-й бит H; p — сумма номеров таблиц MV 2-преобразований, выбранных для j раундов.

Рассмотрим j-й раунд работы схемы. Значение $T_1 = Ctr_1 \oplus H_j^p$ служит начальным значением счетчика для шифрования в режиме CBC:

$$T_i = E_{k\,2}\,(T_{i-1} \oplus S_{i-1}),\ i \in [2,\ m_j],$$

где $E_{k\,2}$ — алгоритм зашифрования AES на ключе k_2.

Вычисляются

$$X_j = N_j \cdot Z_{Nj} \ (\mathrm{mod}\ 256),$$

где $N_j \in [0, 31]$, $Z_{N\,j}$ — N_j-й символ в N_j-й таблице MV 2-преобразования
и раундовый тег

$$Tag_j = \tau(T_{mj},\ X_j),$$

где τ означает циклический сдвиг T_{mj} на 4 бита вправо, когда X_j четное, и аналогичный сдвиг влево, когда X_j нечетное.

После выполнения Nr раундов результирующий тег Tag вычисляется путем сложения по модулю 2 всех раундовых тегов:

$$Tag = Tag_1 \oplus Tag_2 \oplus \ldots \oplus Tag_{Nr}.$$

Таким образом, выход схемы шифрования с аутентификацией является тройкой (C, F, Tag). По одному каналу отправляется пара (C, Tag), по другому — F.

Алгоритм расшифрования с аутентификацией для проверки аутентичности сообщения сначала расшифровывает пришедшие по каналу шифртексты C и F. Затем с помощью расшифрованных значений на каждом раунде по такому же принципу, как в схеме шифрования с аутентификацией, вычисляет раундовые теги, а затем, после выполнения всех раундов вычисляет результирующий тег. Если пришедший по каналу тег аутентификации совпадает с тегом, вычисленным после расшифровки шифртекстов, то проверка целостности выполнена, и выходом алгоритма расшифрования с аутентификацией является исходный текст x. Если же теги не совпали, то алгоритм выдает сообщение об ошибке.

Описанная выше модель программно реализована на языке *C*++ с использованием библиотеки NTL [14]. Приведем пример входных и выходных данных, полученных в результате работы программы.

Входные данные: открытый текст X, нонс N, ассоциированные данные H, ключи k_1 и k_2:

X = [Погасло дневное светило;
На море синее вечерний пал туман.
Шуми, шуми, послушное ветрило,
Волнуйся подо мной, угрюмый океан.]

N = [0×11, 0×01, 0×22, 0×13, 0×04, 0×67, 0×06, 0×17, 0×08, 0×29, 0×0a, 0×61, 0×1c, 0×0d, 0×0e, 0×0*f*];

H = [0×75, 0×11, 0×02, 0×03, 0×07, 0×20, 0×06, 0×16, 0×18, 0×09, 0×0a, 0×0b, 0×0c, 0×23, 0×01, 0×11];

k_1 = [0×9e, 0×47, 0×31, 0×c5, 0×49, 0×ff, 0×58, 0×41, 0×3f, 0×7d, 0×89, 0×e3, 0×11, 0×fb, 0×89, 0×13];

k_2 = [0×15, 0×11, 0×42, 0×30, 0×44, 0×05, 0×06, 0×07, 0×27, 0×19, 0×2a, 0×0b, 0×0c, 0×0d, 0×0e, 0×1*f*].

Выходные данные: шифртексты C и F, тег аутентификации Tag:

C = [±$wДўЗЖ~¶Ђns€6qI{Л@–H€z¬33шэ*0©|_BYµ)
{•zJ§/}§нњMHџBHg~9†Ў6M–WPAI©mшђ!‘Є±#юSЌзhФkя`Ц];

F = [AЬ-©W qR·AeQBM•KCэdЖЬHoIk"п a];

Tag = [“□„™v\OЪMZDй□ШM№].

Заключение. Для организации защищенного документооборота построена модель, обеспечивающая конфиденциальность и целостность обрабатываемых данных. Модель основана на принципах распределенной передачи данных и использования дополнительных ассоциированных данных. Представленная модель программно реализована на языке С++ с использованием библиотеки NTL. Приведены результаты работы программы для тестовых входных данных.

Авторы выражают искреннюю признательность А. Э. Маевскому за полезное обсуждение постановки задачи.

Библиографический список

1. Саттон, М.-Дж.-Д. Корпоративный документооборот: принципы, технологии, методология внедрения / М.-Дж.-Д. Саттон. — Санкт-Петербург : Азбука, 2002. — 448 с.

2. Бабаш, А. В. Криптография / А. В. Бабаш, Г. Р. Шанкин. — Москва : СОЛОН-Р, 2002. — 512 с.

3. Rogaway, P. Evaluation of Some Blockcipher Modes of Operation [Электронный ресурс] / P. Rogaway. — Режим доступа: http://web.cs.ucdavis.edu/~rogaway/papers/modes.pdf (дата обращения 01.06.15).

4. Bellare, M. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm / M. Bellare, C. Namprempre // Lecture Notes in Computer Science. — 2000. — Vol. 1976 : Advances in Cryptology — ASIACRYPT 2000 / ed. T. Okamoto. — Berlin ; Heidelberg : Springer-Verlag, 2000. — P. 531–545.

5. Rogaway, P. Authenticated-encryption with associated-data / P. Rogaway // ACM Conference on Computer and Communications Security (CCS'02). — Washington, 2002. — P. 98–107.

6. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. — Москва : Триумф, 2002. — 816 с.

7. Мищенко, В. А. Ущербные тексты и многоканальная криптография / В. А. Мищенко, Ю. В. Виланский. — Минск : Энциклопедикс, 2007. — 292 с.

8. Мищенко, В. А. Криптографический алгоритм MV 2 / В. А. Мищенко, Ю. В. Виланский, В. В. Лепин. — Минск : Энциклопедикс, 2007. — 176 с.

9. Деундяк, В. М. О стойкости кодового зашумления к статистическому анализу наблюдаемых данных многократного повторения / В. М. Деундяк, Ю. В. Косолапов // Моделирование и анализ информационных систем. — 2012. — Т. 19, № 4. — С. 110–127.

10. Могилевская, Н. С. Программное средство логической проверки корректности криптографических протоколов распределения ключей на основе BAN-логики / Н. С. Могилевская // Вестник Дон. гос. техн. ун-та. — 2012. — Т. 12, № 1, вып. 2. — С. 5–15.

11. Могилевская, Н. С. Пороговое разделение файлов на основе битовых масок: идея и возможное применение / Н. С. Могилевская, Р. В. Кульбикаян, Л. А. Журавлев // Вестник Дон. гос. техн. ун-та. — 2011 — Т. 11, № 10. — С. 1749–1755.

12. Баричев, С. Г. Основы современной криптографии / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. — Москва : Горячая линия — Телеком, 2002. — 176 с.

13. Основы криптографии / А. П. Алферов [и др.]. — Москва : Гелиос АРВ, 2002. — 480 с.

14. NTL: A Library for doing Number Theory [Электронный ресурс] / Victor Shoup. — Режим доступа: http://www.shoup.net/ntl/ (дата обращения 01.06.15).

References

1. Satton, M.G.D. Korporativnyy dokumentooborot: printsipy, tekhnologii, metodologiya vnedreniya. [Corporate document management: principles, technologies, implementation methodology.] St. Petersburg: Azbuka, 2002, 448 p. (in Russian).

2. Babash, A.V., Shankin, G.R. Kriptografiya. [Cryptology.] Moscow: SOLON-R, 2002, 512 p. (in Russian).

3. Rogaway, P. Evaluation of Some Blockcipher Modes of Operation. Available at: http://web.cs.ucdavis.edu/~rogaway/papers/modes.pdf (accessed: 01.06.15).

4. Bellare, M., Namprempre, C. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. Lecture Notes in Computer Science, 2000, vol. 1976, pp. 531–545; Advances in Cryptology — ASIACRYPT 2000, Okamoto, T., ed. Berlin: Springer-Verlag, 2000.

5. Rogaway, P. Authenticated-encryption with associated-data. ACM Conference on Computer and Communications Security (CCS'02). Washington, 2002, pp. 98–107.

6. Shnayer, B. Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si. [Applied Cryptography. Protocols, algorithms, source code in C.] Moscow: Triumf, 2002, 816 p. (in Russian).

7. Mishchenko, V.A., Vilanskiy, V.A. Ushcherbnye teksty i mnogokanal'naya kriptografiya. [Defective texts and multichannel cryptology.] Minsk: Entsiklopediks, 2007, 292 p. (in Russian).

8. Mishchenko, V.A., Vilanskiy, V.A., Lepin, V.V. Kriptograficheskiy algoritm MV 2. [Cipher algorithm.] Minsk: Entsiklopediks, 2007, 176 p. (in Russian).

9. Deundyak, V.M., Kosolapov, Y.V. O stoykosti kodovogo zashumleniya k statisticheskomu analizu nablyudaemykh dannykh mnogokratnogo povtoreniya. [On the firmness code noising to the statistical analysis of the observable data of repeated repetition.] Modelirovanie i AnalyzInformatsionnykh Sistem, 2012, vol. 19, no. 4, pp. 110–127 (in Russian).

10. Mogilevskaya, N.S. Programmnoe sredstvo logicheskoy proverki korrektnosti kriptograficheskikh protokolov raspredeleniya klyuchey na osnove BAN-logiki. [Software tool for logical validation of cryptographic key generation protocols based on BAN-logic.] Vestnik of DSTU, 2012, vol. 12, no. 1, iss. 2, pp. 5–15 (in Russian).

11. Mogilevskaya, N.S., Kulbikayan, R.V., Zhuravlev, L.A. Porogovoe razdelenie faylov na osnove bitovykh masok: ideya i vozmozhnoe primenenie. [Threshold file sharing based on bit masks: concept and possible use.] Vestnik of DSTU, 2011, vol. 11, no. 10, pp. 1749–1755 (in Russian).

12. Barichev, S.G., Goncharov, V.V., Serov, R.E. Osnovy sovremennoy kriptografii. [Fundamentals of modern cryptology.] Moscow: Goryachaya liniya — Telekom, 2002, 176 p. (in Russian).

13. Alpherov, A.P., et al. Osnovy kriptografii. [Fundamentals of cryptology.] Moscow: Gelios ARV, 2002, 480 p. (in Russian).

14. Shoup, V. NTL: A Library for doing Number Theory. Available at: http://www.shoup.net/ntl/ (accessed: 01.06.15).

Поступила в редакцию 05.06.2015
Сдана в редакцию 10.06.2015
Запланирована в номер 24.09.2015